# Information Assurance Metrics: Prophecy, Process, or Pipedream?

Panel Chair: Ronda R. Henning, Harris Corporation
Panelists: Michael J. Skroch, DARPA
John McHugh , Carnegie Mellon Center for Survivable Systems
John Michael Williams, JMW Trading Company

## Session Abstract

Information Assurance has long been considered a "black art" -- a good security engineer knows a good security design or implementation by intuition, not by quantifiable measures. The concept of Information Assurance Metrics endeavors to make information assurance a quantifiable system characteristic, one that can be automatically measured or instrumented. This approach would allow the assurance properties of a system to be analyzed much like more traditional software complexity, test case coverage, and productivity measures. DARPA has initiated the Information Assurance Metrics program to perform the basic science required to support the development of information assurance metrics, processes, and methodologies.

A similar consideration has been the concept of substituting good security processes for good security mechanisms. The move to outsourcing of managed environments has resulted in the concept of service level agreements. In a service level agreement based system, a customer can purchase some level of assurance for his managed applications by stipulating the processes a service provider must have in place on his system.

In both of these cases, the desire for measurable, quantifiable information assurance is present. The question is simple: is it possible to take the qualitative nature of information assurance and transform it into a meaningful set of quantitative measurements? Software engineering has conducted similar activities, with the objective of producing "better" software with fewer defects. Research studies in software engineering over the years have resulted in documented improvements in software productivity and quality.

This panel seeks to present four perspectives on information assurance measurement:

- The perspective of information assurance metrics being attainable in the near term, if a disciplined, scientific approach is applied to the problem.
- The perspective that service level agreements provide a near term approach to determining the information assurance capabilities of a service provider.
- The perspective of useful assurance processes with the use of auditing to ensure process execution, with the realization these assurance processes will never replace good, basic assurance mechanisms.
- The perspective of the information assurance community learning from the software engineering disciplines and their repeated attempts to turn good software development practices into a quantitative measurement-based science before information assurance metrics take a similar path.

# Panel Position Paper- Information Assurance Metrics: Prophecy, Process, or Pipedream?

John McHugh - jmchugh@cert.org
Carnegie Mellon Center for Survivable Systems

"*Systems that can be attacked at the register level must be protected at the register level.*" - Earl Boebert

"*If anything can go wrong, it will.*" - Murphy

In recent years, DARPA has been urging the application of the scientific method to a number of problems areas in information assurance and computer security. The push to develop quantifiable measures of assurance is but one step in this progression. While the goals of this movement are laudable, the underlying science is sadly lacking. Software development is, at best, in the craft era. The state of practice, as typified by commercial products such as Windows and many of its (too) closely integrated applications is abominable.

I would like to believe that metrics relating to security are possible, but there is little evidence to support this view at present. First, let us consider what a security metric might measure. There are several candidates - a measure of the resources or effort required to compromise the system is the most obvious. For such a measure to be useful, it should be soundly based on demonstrable assurances of the form "If I do **X** (at cost **Y**) the cost of compromising the system will be raised by **Z**." This kind of metric is clearly applicable to security measures such as properly managed crypto systems, but fails to take Murphy into account. Cathy Meadows has recently introduced a work factor concept into the analysis of cryptographic protocols for denial of service vulnerabilities, a step in the right direction that might be applicable elsewhere. It might be interesting to consider the effort required to discover a vulnerability and develop an exploit for it as well as the effort to deploy the exploit. Unfortunately, for commodity systems, our failure to heed Boebert makes the former fairly modest (and easily amortized over repetitions of the exploit) while the latter is usually trivial. Most of our deployed systems are patently insecure and the value that could be assigned to any work factor metric for compromising them is vanishingly small.

The TCSEC and subsequent evaluation criteria are based on an assumption that process plus technology gives demonstrable assurance, but there is little evidence to support this view, and even so, much of the applicable assurance technology is out of vogue. Even the SW-CMM community is more comfortable in measuring process related attributes such as cost and productivity as opposed to attributes, such as reliability, that might be related to security. Although many of the DoD software development contractors have had CMM evaluations, neither Microsoft nor any of the major Unix providers appear to have been evaluated. On a smaller organizational scale, the PSP/TSP approach to individual and team skills building appears to bring about a dramatic reduction in software defects, but to date, there is no experience with security relevant defects. It is

likely that some combination of PSP/TSP with training in secure coding practices would lead to systems that avoid many of the blunders common in commodity software today. If the result was an reduction in security related flaws to the point that significant work factors were required to discover new vulnerabilities, it might be possible to substantiate a work factor / process link and approach metrics from the process viewpoint.

Even if we learn to heed Boebert and build systems that have substantial resistance to frontal assaults, Murphy is likely to confound our results. There is evidence that poor system management and operational practices are an enabling factor in many compromises. Work factor measures assume that doing the work is the only way to breach the system. If the likelihood that the attacker can find an easier way to effect a compromise is fairly high, the work factor required by the brute force approach is irrelevant. I am even less sanguine about developing measures for effective system administration, security management, etc. than I am about work factor based measures based on assurance techniques.

# Panel Position Paper - Information Assurance Metrics: Prophecy, Process or Pipedream?

John Michael Williams

1) The State of the Art ...

at NIST, DoD, DoE (unclassified), GAO, USAID, USDA, Customs, Bear-Stearns, Citigroup, First Union, Dupont, General Motors et al. (A)

--- sorry as it can be ...

2) Security is an emergent property, capable of emerging only from the best-quality products.

3) A source despised by some [nerds and geeks?] says: "[C]omputers are 'crap'... They are the lowest-quality major purchase you can buy... Most companies couldn't get away with shipping something with known defects. But their whole attitude is, it's very complicated, it's cutting edge, it's very cool, and if there's 16 things wrong, we're going to ship it anyway. It's the science-project mentality: You're all my guinea pigs." (B)

4) Ergo, security measures will for the foreseeable future encourage confidence when and where there should be none, and are a waste of valuable resources.

Lucent's new Class 5 voice-network switch availability rating of 99.9999 means that this hardware experiences about 10 seconds of downtime per year. (C)

That's a real number. But none of us will ever have six 9s of security.

---

(A) Workshop on "Approaches To Measuring Security," Computer System Security and Privacy Advisory Board, NIST, Gaithersburg MD, 6/13-14/00. http://csrc.nist.gov/csspab/

(B) Walter Mossberg, Wall Street Journal Personal Technology Editor http://ptech.wsj.com/, in "Curmudgeon on the Info Highway," Howard Kurtz, Washington Post pg A1, 6/24/00 http://www.washingtonpost.com/wp-dyn/articles/A52395-2000Jun23.html

(C) Interactive Week, 5/24/00, http://www.zdnet.com/intweek/stories/news/0,4164,2574575,00.html

---

# Panel Position Paper - Information Assurance Metrics: Prophecy, Process or Pipedream?

Michael J. Skroch

Inherent problems exist in the current design and assessment processes that create our information systems. To address these problems a new information assurance (IA) paradigm is required – one that enables the designer and analyst to capture and probe the causality, relationships, and objectives of an entire system. DARPA's IA Science and Engineering Tool (IASET) program is addressing the IA problem by developing this new paradigm. We are developing underlying sciences that will allow us to formally understand the problem at hand and developing an environment and tools that designers and assessors can use to solve real IA problems, assess competing IA strategies and mission impact, and reduce risk. A key aspect of approach is scientifically identifying and understanding IA metrics.

Metrics are standard measures one chooses to use to specify and record a current situation, compare it to similar past measures, and make decisions through figures of merit. No current universally accepted metrics for measuring and assessing the effectiveness of IA exist. Metrics exist in many categories and may embody many properties. For instance, they range between qualitative and quantitative. While it may be desirable to reduce all metrics to numeric values, we should be careful not to immediately force qualitative or non-numeric metrics to such a scale for fear of loosing information or reducing their utility. Our goal is to first identify metrics that are measurable, testable, and useful for IA and then move as many of these as far as possible toward the quantitative side of the scale. Where metrics are qualitative, we must at least provide a common frame of reference and language so that common understanding exists between designer, assessors, and operators.

Metrics are vital for the quantification and comparison of assurance components over time, comparison between similar systems, comparison to requirements, and as a measure of utility for a system in a particular environment.

The ultimate objective is to produce useful metrics for designers, assessors, planners, and users. We should consider development of metrics from both the user's point of view and from the base cyberscience that underlies the field of IA. Metrics that by nature are abstract may be of no value to the user but may be necessary to advance the area of IA. Closely related to metrics is the concept of benchmarks or touchstones for IA. Metrics provide standards of measure but may not provide insight, which humans can readily understand and utilize. IA will have to develop comparative benchmark metrics, measured against a standard scale, because absolute metrics will not always be available. If the metrics we identify are to be used to address a system problem, if they are to be used from specification through design, assessment and operational deployment, their meaning must be consistent and defined. We must provide an integrated environment for metrics by defining their purpose, meaning, units, range of values, inherent taxonomies, and relationship to other metrics and calculations for IA.

Author: Michael Skroch, Program Manager, Information Assurance Science and Engineering Tools (IASET), Defense Advanced Research Projects Agency (DARPA), Information Systems Office (ISO), mskroch@darpa.mil, 703-696-2375.

### Background of the Audience

This presentation should be of interest to three distinct groups:

1. Information assurance researchers, who are exploring the measurement of assurance in system components and complex systems.
2. Information assurance practitioners, who will have to learn to live with the tools and methodologies from information assurance research.
3. Information assurance consumers, who are in search of succinct, meaningful ways to express their assurance requirements that are comprehensible to their constituent organizations.

All three groups can benefit from aspects of this discussion, as we attempt to evolve from the black art of information assurance to a structured, scientific discipline.

## Panel Member Biographies

Ronda Henning is the senior Secure Systems Engineer for Harris Corporation, Government Communications Systems Division; a Melbourne, Florida based international communications and electronics company. Ms. Henning currently leads the Information Assurance center of excellence responsible for information assurance technology research and development as well as assurance technology insertion large scale systems integration opportunities. Prior to her employment at Harris, Ms. Henning was a deputy branch chief of information security research and development at the National Security Agency. A Certified Information Systems Security Professional (CISSP), she holds an M.B.A. from the Florida Institute of Technology, an M.S. in Computer Science from Johns Hopkins University, and a B.A. from the University of Pittsburgh.

John McHugh is a senior member of the technical staff at CERT, part of the SEI at CMU. He was a professor and former chairman of the Computer Science Department at Portland State University in Portland, Oregon where he held a Tektronix Professorship. His research interests include computer security, software engineering, and programming languages. He has previously taught at The University of North Carolina and at Duke University. He has been an active researcher in the application of formal methods to the construction of dependable and secure systems for many years. He was the architect of the Gypsy code optimizer and the Gypsy Covert Channel Analysis tool. Dr. McHugh received his PhD degree in computer science from the University of Texas at Austin. He has a MS degree in computer science from the University of Maryland, and a BS degree in physics from Duke University. He grew up in Durham, North Carolina, leaving when he graduated from Duke. Twenty years later, he returned, demonstrating that Thomas Wolfe was wrong. After another ten years in Durham, he moved to Portland, demonstrating, perhaps, that Wolfe knew what he was talking about after all.

John Michael (Mike) Williams spent more than 24 years with Unisys, 8 years with CSC and several with other companies from 1956 to 1993. He has been in every aspect of security since 1973, and a specialist in security R&D since 1977, first addressing security metrics for nuclear-warfare command and control (WWMCCS) in the late '70s. He has been independent since 1993, advising a wide range of domestic and international defense contractors, computer makers and startups in wireless telecommunications and Internet services. He can be reached at John.Michael.Williams@Computer.org.

Michael J. Skroch (skraw) is a Program Manager at the Defense Advanced Research Projects Agency (DARPA), Information Systems Office (ISO) where he manages two programs. The Information Assurance Science and Engineering Tools (IASET) program, which focuses on cyberscience, IA engineering, and malicious code mitigation, is scheduled to run through FY 2003. The Information Assurance (IA) program, which addresses a broad set of IA capabilities such as trust composition, is scheduled to run through FY 2000. These are two of eight programs in the Information Assurance and Survivability (IA&S) program suite at DARPA. Michael is a member of the Infosec Research Council (IRC), which coordinates Information Assurance and security research across multiple government agencies. Previously, at Sandia National Laboratories in Albuquerque, New Mexico, he was involved in various national security projects for the DOE, DOD, DOS, and other agencies in the area of systems design and vulnerability assessment for information security including electromagnetic pulse, High Altitude Electromagnetic Pulse, and TEMPEST. He was involved with formalization of information systems surety red teaming and infrastructure surety assessment efforts and established a red teaming capability for these areas. He has worked on various nuclear command and control projects for USSTRATCOM, USSPACECOM, and USPACOM. Michael also worked at Calspan Corporation (now Veridian Engineering), Communication Satellite Corporation (COMSAT) and IBM at Research Triangle Park. .Michael earned his Bachelor of Science in Electrical Engineering at the Rochester Institute of Technology and his Master of Science in Electrical Engineering at the University of Wisconsin-Madison where he focused on control and information theory.

Michael J. Skroch
Program Manager
Information Systems Office
Defense Advanced Research Projects Agency
3701 N. Fairfax Dr.
Arlington, VA 22203
voice: 703-696-2375
email: mskroch@darpa.mil
web: http://www.darpa.mil/iso/
web: http://www.iaset.org/
web: http://www.iaands.org/